MISE EN CONFORMITÉ AU RGPD

L'ÉTAT D'AVANCEMENT DES ÉTABLISSEMENTS FINANCIERS

Nicolas Vetriak

Associé

Novaminds

Gaël Duval

Directeur

Novaminds

Cédric Frenel

Avocat associé

Courtois Lebel

Les établissements financiers seront-ils prêts en mai prochain, lors de l'entrée en vigueur du Règlement général sur la protection des données (RGPD) ? L'enquête menée par Novaminds fait état d'un avancement des chantiers à mener dans cette perspective : organisation du dispositif, gouvernance, inventaire des traitements, nouveaux processus, revue des contrats avec les sous-traitants, traitement des impacts sur le SI... et identifie les freins rencontrés.

Le RGPD entrera en vigueur en mai prochain. Les établissements financiers, banques ou entreprises d'assurances, seront-ils prêts à cette date ? Novaminds a réalisé une nouvelle édition de son enquête de place sur la Gouvernance de la donnée et de sa Protection et a, dans ce cadre, au moyen d'entretiens approfondis, dressé à fin 2017 un état d'avancement des programmes de mise en conformité. L'enquête s'est déroulée auprès d'un panel de 17 établissements financiers de tailles et d'activités diverses. Cette enquête a été l'occasion de dresser un état des lieux des programmes (banque, assurance et groupe de protection sociale), des démarches de mise en conformité et de déterminer les grandes tendances qui commencent à se dessiner autour de la fonction de DPO et des futurs chantiers sur la protection des données à caractère personnel.

I. État des lieux

Si seule la moitié des entreprises du panel avait engagé un programme global de mise en conformité lors de l'édition 2016 de l'enquête Novaminds, à fin 2017, les établissements sont en ordre de marche : ils ont effectué le cadrage de leur programme et engagé les actions de mise en conformité au RGPD. Pour autant, cet effort général cache des disparités. L'état d'avancement reste inégal d'une entreprise à l'autre, le cadrage s'étant pour certaines entreprises tout juste terminé au deuxième semestre 2017, alors que d'autres annoncent un avancement conforme aux objectifs. Le cadrage porte généralement sur :

– la réalisation d'une analyse d'écart entre l'existant et les exigences du texte ;
– la détermination des actions à mener pour couvrir ces écarts ;
– la définition de l'organisation, des rôles et des responsabilités à mettre en place pour les mener ;
– la détermination des moyens humains et financiers nécessaires.

L'allongement des délais de la phase de cadrage s'explique le plus souvent par la difficulté à identifier un sponsor au sein de l'organisation, la sous-estimation des impacts du programme sur les processus, systèmes et organisations existants et, dans certains cas, le temps nécessaire à la désignation du DPO en préalable au lancement effectif du programme.

L'avancement constaté peut aussi être très disparate au sein d'un même groupe entre les différentes entités ou en fonction des chantiers ouverts dans le cadre de préparation à l'entrée en vigueur du RGPD. Chaque entreprise a structuré son programme en fonction de sa situation et de son organisation existante mais, globalement, les grands chantiers sont les suivants :

– **la définition de l'organisation** comprenant le dispositif de premier niveau qui sera chargé de l'exécution opérationnelle des processus impactés ou requis par le nouveau règlement (gestion du registre des traitements, recueil du consentement…) et le dispositif de second niveau chargé du contrôle de la conformité globale du dispositif par rapport au règlement. Le second niveau comprend notamment la nomination du *Data Protection Officer* (DPO), acteur clé du dispositif qui devra notamment, informer et conseiller le plus haut niveau de la direction de l'entreprise, mais aussi l'ensemble des collaborateurs, coopérer et être le point d'entrée unique vis-à-vis de l'autorité (CNIL ou autorité chef de file) et s'assurer de la conformité du dispositif et des mesures de protection mises en place par rapport aux exigences réglementaires ;
– **le déploiement de la gouvernance** et notamment la mise à jour des nombreuses politiques, procédures et processus impactés par le RGPD, ainsi que la création de nouvelles politiques et procédures dédiées à la gestion des données à caractère personnel, à leur usage au sein des processus et systèmes de *reporting* et d'exploitation de données ;
– **l'inventaire des traitements** de données à caractère personnel et la constitution du registre des traitements qui peut être construit soit en complétant le registre des traitements existant lorsque l'entreprise disposait d'un CIL (Correspondant Informatique et Libertés), soit en réalisant un inventaire complet des traitements, ce qui nécessitera des travaux de plus grande ampleur ;

« À fin 2017, les établissements sont en ordre de marche : ils ont effectué le cadrage de leur programme et engagé les actions de mise en conformité au RGPD. »

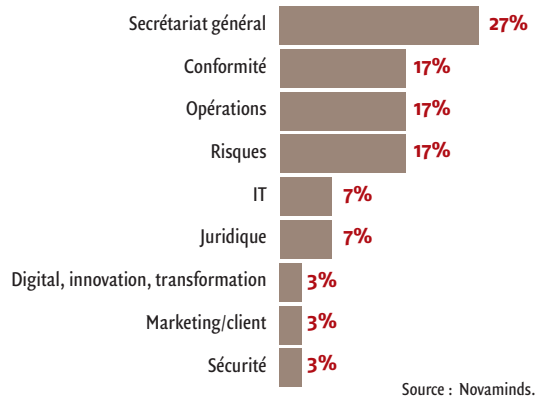
– **la mise en place de nouveaux processus** pour répondre aux dispositions réglementaires permettant aux personnes d'exercer leurs droits. Même si un certain nombre de droits préexistaient dans les réglementations déjà en place, le RGPD a été l'occasion, pour beaucoup d'entreprises, de faire le constat que les dispositifs en vigueur n'étaient pas adaptés ou complets. Le RGPD introduit des renforcements majeurs des droits des personnes (confirmation du droit à l'oubli, renforcement du consentement explicite…) ainsi que l'introduction de nouveaux droits (portabilité…) qui nécessitent la mise en place de nouveaux processus ;
– **la revue des contrats** avec les sous-traitants manipulant des données à caractère personnel afin d'y introduire des clauses spécifiques fixant leurs responsabilités et notamment de garantir une sécurité suffisante des données personnelles en mettant en œuvre les mesures de protection nécessaires. Suivant le degré d'externalisation des activités manipulant des données à caractère personnel, ce chantier peut s'avérer très important. Au-delà des contrats avec les sous-traitants, le RGPD impose aussi potentiellement une revue des contrats avec les clients. D'une manière plus générale, une révision des relations avec les tiers internes et externes dont les données à caractère personnel sont échangées et manipulées ;
– **le traitement des impacts sur le système d'information** (SI) et la mise en place ou le renforcement des mesures de protection et de sécurisation des données à caractère personnel. Ces travaux sont délicats à mener car ils nécessitent de disposer d'une parfaite connaissance du SI existant et se heurtent souvent à un existant informatique qui ne permet pas la mise en place aisée des exigences du RGPD. La mise en place des mesures de protection et de sécurisation des données à caractère personnel exige aussi généralement une adaptation des standards de sécurité en vigueur afin d'y intégrer les exigences de respect de la vie privée (*privacy by design/by default*), cela étant pris en charge le plus souvent dans les programmes de Cyberdéfense également en cours de mise en œuvre ;
– **la communication et la sensibilisation** aux nouvelles dispositions introduites par le RGPD au travers de la conduite d'actions visant l'ensemble des collaborateurs et de plans de formation destinés aux acteurs directement impliqués dans le dispositif (collaborateurs manipulant des don-

nées à caractère personnel, acteurs de la fonction DPO, correspondants Protection des données...).

Les chantiers de déploiement de la gouvernance, de l'organisation et du registre des traitements sont les plus avancés et seront globalement achevés à mai 2018 pour les entreprises les plus en pointe. L'explication est double :

– cette focalisation des entreprises sur ces trois chantiers constitue la démarche la plus courante pour être en mesure d'assurer un niveau de conformité minimum pour l'échéance de mai. Sur les autres chantiers, l'approche consiste généralement à assurer une mise en conformité uniquement sur les traitements évalués comme les plus sensibles au regard du texte. Cela correspond du reste à l'approche par les risques prônée par le règlement ;

1. POSITIONNEMENT DES SPONSORS (FIN 2017)



Source : Novaminds.

– l'avancement global sur ces trois chantiers est plus important pour les assurances que pour les établissements bancaires. Les assurances disposaient déjà majoritairement d'une organisation et d'une gouvernance en place dans le cadre de la réglementation Informatique et Libertés et d'un registre des traitements. Dans ces conditions, ces chantiers ont principalement consisté à adapter, sans effort significatif, le dispositif existant.

SPONSORS ET RESPONSABLE DU PROGRAMME RGPD

En termes de positionnement des sponsors et du responsable du programme RGPD, quatre schémas peuvent être identifiés :

– le programme est placé sous la responsabilité du CIL avec un sponsorship de la fonction conformité, ou juridique, ou encore du secrétariat général. Ce schéma concerne surtout les entreprises d'assurance qui disposaient déjà d'un CIL contrairement à la majorité des établissements bancaires ;

– le programme est placé sous la responsabilité de la fonction sécurité lorsque celle-ci est positionnée au sein de la direction des risques ou de la conformité ;

– la responsabilité est assurée par les CDO[1] lorsque ceux-ci avaient déjà dans leurs missions des programmes réglementaires sur la donnée (BCBS239). Ce schéma concerne exclusivement des établissements bancaires ;

– la responsabilité est assurée par des chargés de programmes spécifiques.

L'évolution du programme et notamment la nomination du DPO ont, dans la plupart des cas, impacté ces choix d'organisation initiaux. Le DPO, une fois nommé, a été intégré au programme et a souvent pris en charge les chantiers relatifs à l'organisation de la filière protection des données personnelles. Cette filière devant constituer, à l'issue du programme, le réseau de correspondants, de relais et d'experts sur lequel le DPO pourra s'appuyer pour mener à bien ses missions. Le sponsorship des programmes a lui aussi évolué pour intégrer les directions impliquées dans le mode « Run » et notamment la direction d'appartenance du DPO.

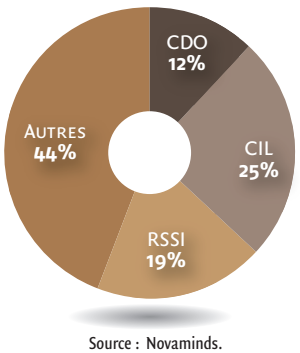
II. Les questions soulevées par la mise en œuvre de ces chantiers

Une des principales questions soulevées dans le cadre des programmes de mise en conformité est celle du positionnement du DPO.

Le DPO est dans la plupart des cas positionné au sein de la fonction conformité ou au sein de la fonction juridique, compte tenu des compé-

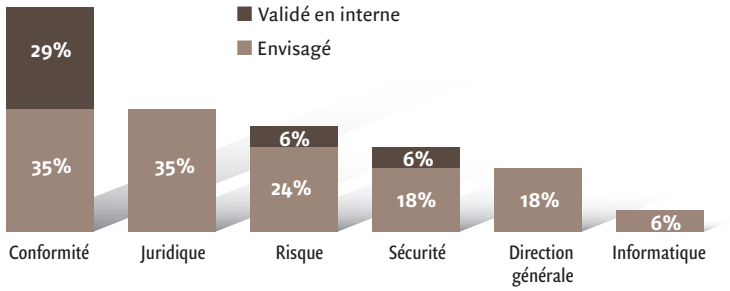
[1] *Chief Data Officer.*

2. RESPONSABILITÉ DES PROGRAMMES (FIN 2017)



Source : Novaminds.

3. LES SCHÉMAS DE POSITIONNEMENT DES DPO GROUPE (FIN 2017)



Source : Novaminds.

tences requises et de l'implication de cette fonction dans le cadrage initial du programme. Le rattachement à la fonction sécurité est aussi parfois envisagé du fait de l'adhérence des missions du DPO avec les mesures de protection des données et dans les cas où la fonction sécurité n'est pas intégrée dans la fonction informatique. Enfin, certains établissements envisagent un rattachement à la fonction risque ou directement à un membre de la direction générale. Les schémas de déploiement de la communauté des DPO étaient à fin 2017 pour la plupart des établissements encore en cours de réflexion, mais quatre schémas d'organisation se dégagent :

– un DPO groupe assurant les missions réglementaires et s'appuyant sur des relais internes par pays, entités juridiques ou fonctions ;

– un DPO groupe assurant l'animation et la coordination de relais locaux de chaque entité ou pays, qui prennent en charge les missions réglementaires ;

– un DPO groupe unique sans relais locaux ;

– un réseau de DPO locaux sans DPO groupe.

DES DIFFICULTÉS OPÉRATIONNELLES

Enfin, certaines difficultés opérationnelles ont émergé des exigences du règlement :

– la détermination des durées de conservation des données ainsi que la mise en œuvre des purges au sein du SI. Celles-ci exigent de déterminer de façon consensuelle, pour tous les métiers et tous les pays d'un groupe, la durée de conservation d'une donnée. Contrairement au RGPD qui s'applique uniformément sur l'ensemble des pays européens, les durées de conservation restent bien souvent variables : en fonction de la réglementation de chaque pays ; en fonction des différentes réglementations applicables pour un même pays ;

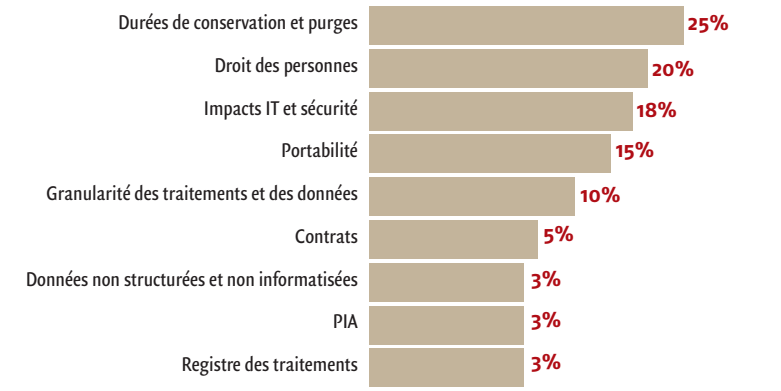
– la mise en œuvre de la purge des données est un autre obstacle : elle se heurte bien souvent à sa faisabilité technique au sein d'un SI existant hétérogène et complexe, qui n'a pas été conçu pour mettre en œuvre de façon transversale ce type de principe ;

– plus globalement, l'implémentation des mesures de sécurité et l'ensemble des impacts du RGPD sur le SI sont ressentis comme une vraie difficulté. Pour beaucoup d'entreprises, ces chantiers nécessitent des investissements d'ampleur visant à transformer les systèmes et les infrastructures informatiques et s'étaleront dans le temps, bien au-delà de l'échéance du 25 mai 2018. Par ailleurs, la mise en œuvre de ces mesures de sécurité s'inscrit souvent dans le cadre des programmes de Cyberdéfense dont les priorités et le calendrier ne sont pas toujours cohérents avec les exigences du RGPD ;

– la mise en œuvre opérationnelle des processus permettant de gérer les droits des personnes : parmi les thématiques les plus délicates, la nécessité du recueil du consentement explicite dans le cas de profilage est régulièrement évoquée. À noter que ce sujet, évoqué mi-2017 par beaucoup des entreprises du panel, a fait l'objet de clarifications de la part du G29 durant le mois d'octobre 2017 ; Autre difficulté souvent citée, la déclinaison opérationnelle de la portabilité notamment en raison de l'incertitude concernant le périmètre des données concernées ;

– par ailleurs, certaines entreprises du panel anticipent déjà que la mise en place opérationnelle de la gestion des droits, l'enregistrement des demandes des personnes concernées ainsi que la capacité à pouvoir justifier leur bonne application nécessiteront, compte tenu du volume potentiellement énorme de demandes, une automatisation et un outillage spécifique.

4. EXIGENCES DU GRPD LES PLUS DIFFICILES À COUVRIR (FIN 2017)



Source : Novaminds.

« Le DPO est dans la plupart des cas positionné au sein de la fonction conformité ou au sein de la fonction juridique, compte tenu des compétences requises et de l'implication de cette fonction dans le cadrage initial du programme. »

En raison du manque de maturité des solutions informatiques du marché et de l'ampleur du projet, ce chantier nécessitera du temps et s'étalera également, probablement, bien au-delà de l'échéance du 25 mai 2018 ;

– la question de la granularité des traitements est moins citée par les établissements, mais pose des interrogations structurantes pour tout le

« Parmi les thématiques les plus délicates, la question de la nécessité du recueil du consentement explicite dans le cas de profilage est régulièrement évoquée. »

programme de mise en conformité. Les *Guidelines* du G29 ont précisé les éléments nécessaires à une gestion conforme du recueil du consentement et notamment les exigences en termes de granularité, qui supposent un *opt-in* distinct pour chaque type de finalité. On observe cependant au sein du panel de profondes différences d'interprétation et un niveau de granularité très disparate dans la définition de ce que l'on entend par traitement. À titre d'exemple, pour les entreprises de taille et d'activité comparables, le nombre de traitements recensés peut varier de 1 à 10 ;

– la dernière difficulté à mettre en avant est la mise en conformité des traitements sur les données non structurées, non informatisées. Ce point est, de façon surprenante, assez peu cité par les entreprises du panel. Cela ne signifie probablement pas qu'il ne pose pas de difficulté mais que dans l'état d'avancement actuel des programmes, son traitement est reporté après l'échéance de mai 2018 compte tenu de la complexité et de l'ampleur du sujet.

III. Les moyens alloués

Globalement les effectifs dédiés aux programmes de mise en conformité restent difficiles à évaluer, en raison de la forte décentralisation des moyens humains. En effet, la maîtrise et la connaissance des traitements et des données à caractère personnel supposent de positionner les acteurs opérationnels du programme au plus près des métiers, au sein des entités locales opérant les traitements. En conséquence, les moyens humains positionnés au niveau groupe consolidé restent faibles, autour d'une dizaine d'ETP pour la plupart des entreprises. Ces chiffres peuvent bien sûr varier en fonction de l'existant Informatique et Libertés et du caractère fédéraliste ou capitalistique des établissements. Les effectifs positionnés au niveau groupe sont en charge du pilotage du programme et de la coordination globale des travaux, mais n'assurent généralement pas de missions opérationnelles de mise en conformité.

Côté budget, les montants constatés sont très variables. Les plus gros budgets consacrés au RGPD sont de l'ordre de 100 à 120 millions d'euros (montant pluriannuel consolidé au niveau groupe) pour les plus grands établissements financiers. À l'autre bout de l'échelle, des entreprises d'assurance ont fait le choix d'une forte capitalisation sur l'existant Informatique et Libertés, ce qui explique le budget réduit consacré à la mise en conformité.

Le constat global est que l'effort nécessaire à la mise en conformité est ressenti comme beaucoup plus important dans le secteur bancaire que dans le secteur des assurances.

Ces constats s'expliquent par la différence de maturité entre les deux secteurs en termes de protection de la vie privée. En effet et contrairement au secteur bancaire, l'immense majorité des entreprises d'assurance avaient nommé depuis longtemps un Correspondant Informatique et Libertés et déployé une organisation associée, sur l'ensemble du groupe via des relais et correspondants locaux. Elles avaient, par conséquent, mis en place un dispositif de gestion des droits des personnes et un registre des traitements sur les données à caractère personnel. Cette préoccupation déjà ancienne des assureurs quant à la protection des données personnelles est en partie expliquée par la sensibilité particulière des données mises en jeux au sein des activités d'assurance et notamment des données de santé.

Conclusion

Pour la plupart des entreprises, les programmes ne seront pas clos à l'échéance du 25 mai 2018 et se poursuivront bien au-delà. Les raisons principales en sont les difficultés à réaliser un recensement exhaustif des traitements, les impacts du texte sur le SI et les mesures de sécurité, ainsi que les questions que posent la mise en œuvre des durées de conservation, le recueil du consentement et la portabilité.

Au-delà des problématiques posées par le texte, la sous-évaluation chronique des moyens humains et la découverte, au fur et à mesure du déroulement des chantiers, de l'ampleur et de la complexité du sujet n'avaient pas été anticipées initialement. En conséquence, certains établissements envisagent déjà des plans d'action s'étalant sur plusieurs années.

La mise en conformité avec le RGPD exigera l'identification de leviers d'accélération permettant d'optimiser les actions à mener. L'existant Informatique et Libertés, présent majoritairement dans le secteur des assurances, constitue clairement l'un de ces leviers sur lequel les entreprises concernées ont capitalisé. Les autres entreprises se concentrent majoritairement aujourd'hui sur la mise en œuvre de « victoires rapides » permettant d'établir un socle minimum de conformité à l'échéance.

En synthèse, on pensait il y a encore un an que l'essentiel serait en place à l'échéance. On s'aperçoit aujourd'hui que le chemin à parcourir est encore long. ■